What is claimed is:

1. A data usage controlling apparatus that

    (1) reads a type 1 key from a storage unit and

        (a) main data,

        (b) an encrypted type 2 key produced by

encrypting a type 2 key using the type 1 key, and

        (c) encrypted condition information produced

by encrypting condition information using the type

2 key

        from a recording medium,

    (2) decrypts the encrypted condition information

using the type 2 key, and

    (3) controls usage of the read main data based on the

condition information,

    the data usage controlling apparatus comprising:

    first updating means for updating the condition

information in accordance with usage of the read main data;

    generating means for generating a new type 2 key in

accordance with the usage of the read main data;

    first encrypting means for encrypting the updated

condition information using the new type 2 key and

replacing the encrypted condition information on the

recording medium with the encrypted updated condition

information;

    second updating means for updating the type 1 key in

the storage unit in accordance with the usage of the read

main data; and

34

27   second encrypting means for encrypting the new type

28   2 key using the updated type 1 key and replacing the

29   encrypted type 2 key on the recording medium with the

30   encrypted new type 2 key.

1

1   2. A data usage controlling apparatus that

2   (1) reads a type 1 key from a storage unit and a set

3   including

4   (a) main data,

5   (b) an encrypted type 2 key produced by

6   encrypting a type 2 key using the type 1 key, and

7   (c) encrypted condition information produced

8   by encrypting condition information using the type

9   2 key

10   from a recording medium on which n (where n is

11   an integer no less than two) sets of main data, an

12   encrypted type 2 key, and encrypted condition

13   information are recorded,

14   (2) decrypts the encrypted condition information

15   using the type 2 key, and

16   (3) controls usage of the read main data based on the

17   condition information,

18   the data usage controlling apparatus comprising:

19   generating means for generating a new type 2 key in

20   accordance with usage of the main data;

21   first encrypting means for encrypting the condition

22   information using the new type 2 key and replacing the

35

23 encrypted condition information on the recording medium

24 with the newly encrypted condition information;

25   decrypting means for decrypting all (n-1) encrypted

26 type 2 keys on the recording medium that are not included

27 in the read set using the type 1 key;

28   updating means for updating the type 1 key in the

29 storage unit after the decrypting means has decrypted all

30 (n-1) encrypted type 2 keys; and

31   second encrypting means for encrypting the (n-1) type

32 2 keys and the new type 2 key using the updated type 1 key

33 and replacing all n encrypted type 2 keys on the recording

34 medium with the newly encrypted type 2 keys.

1

1 3. A data usage controlling apparatus in accordance with

2 Claim 2, further comprising:

3   second updating means for updating the condition

4 information in accordance with usage of the read main data,

5   wherein the first encrypting means encrypts the

6 updated condition information using the new type 2 key and

7 replaces the encrypted condition information on the

8 recording medium with the encrypted updated condition

9 information.

1

1 4. A data usage controlling apparatus in accordance with

2 Claim 3,

3   wherein the generating means generates a new type 2

4 key every time a user makes a predetermined number of uses

36

5   of the main data on the recording medium, and

6   when the generating means has not generated a new type

7   2 key, the first encrypting means re-encrypts the updated

8   condition information using a same type 2 key as was used

9   to decrypt the encrypted condition information.

1

1   5. A data usage controlling apparatus in accordance with

2   Claim 2,

3   wherein the main data in each set on the recording

4   medium has been encrypted using a type 3 encryption key,

5   the data usage controlling apparatus further

6   comprising:

7   obtaining means for obtaining the type 3 encryption

8   key; and

9   second decrypting means for decrypting the read main data

10 using the obtained type 3 encryption key.

1

1   6. A data usage controlling apparatus in accordance with

2   Claim 2,

3   wherein the main data in each set on the recording

4   medium has been encrypted using a type 3 encryption key

5   that is unique to the data usage controlling apparatus,

6   the data usage controlling apparatus further

7   comprising:

8   storing means for storing the type 3 encryption key;

9   and

10 second decrypting means for decrypting the read main data

11   using the stored type 3 encryption key.

1

1   7. A data usage controlling apparatus in accordance with

2   Claim 2,

3   wherein the updating means updates the type 1 key by

4   performing a predetermined calculation on the read type

5   1 key.

1

1   8. A data usage controlling apparatus in accordance with

2   Claim 2,

3   wherein the updating means updates the type 1 key by

4   adding one to the read type 1 key.

1

1   9. A data usage controlling method that

2   (1) reads a type 1 key from a storage unit and

3   (a) main data,

4   (b) an encrypted type 2 key produced by

5   encrypting a type 2 key using the type 1 key, and

6   (c) encrypted condition information produced

7   by encrypting condition information using the type

8   2 key

9   from a recording medium,

10   (2) decrypts the encrypted condition information

11   using the type 2 key, and

12   (3) controls usage of the read main data based on the

13   condition information,

14   the data usage controlling method comprising the

38

15 following steps:

16   updating the condition information in accordance

17 with usage of the main data;

18   generating a new type 2 key in accordance with the

19 usage of the main data;

20   encrypting the updated condition information using

21 the new type 2 key and replacing the encrypted condition

22 information on the recording medium with the encrypted

23 updated condition information;

24   updating the type 1 key in accordance with the usage

25 of the main data; and

26   encrypting the new type 2 key using the updated type

27 1 key and replacing the encrypted type 2 key on the

28 recording medium with the encrypted new type 2 key.

1

1 10. A computer-readable recording medium storing a program

2 that

3   (1) reads

4   a type 1 key from a storage unit and

5   (a) main data,

6   (b) an encrypted type 2 key produced by

7 encrypting a type 2 key using the type 1 key, and

8   (c) encrypted condition information produced

9 by encrypting condition information using the type

10 2 key

11   from a recording medium,

12   (2) decrypts the encrypted condition information

39

13 using the type 2 key, and

14   (3) controls usage of the read main data based on the

15 condition information,

16   the program including instructions for executing the

17 following processes:

18   updating the decrypted condition information in

19 accordance with usage of the main data;

20   generating a new type 2 key in accordance with usage

21 of the main data;

22   encrypting the updated condition information using

23 the new type 2 key and replacing the encrypted condition

24 information on the recording medium with the encrypted

25 updated condition information;

26   updating the type 1 key in accordance with usage of

27 the main data; and

28   encrypting the new type 2 key using the updated type

29 1 key and replacing the encrypted type 2 key on the

30 recording medium with the encrypted new type 2 key.

31